Microsoft Azure

Azure Networking

Joe Losinski
Partner Technology Strategist

Azure Networking

1 Microsoft Global Network

2 Virtual Machine Networking

3 Key Networking Services

4 Hybrid Connectivity

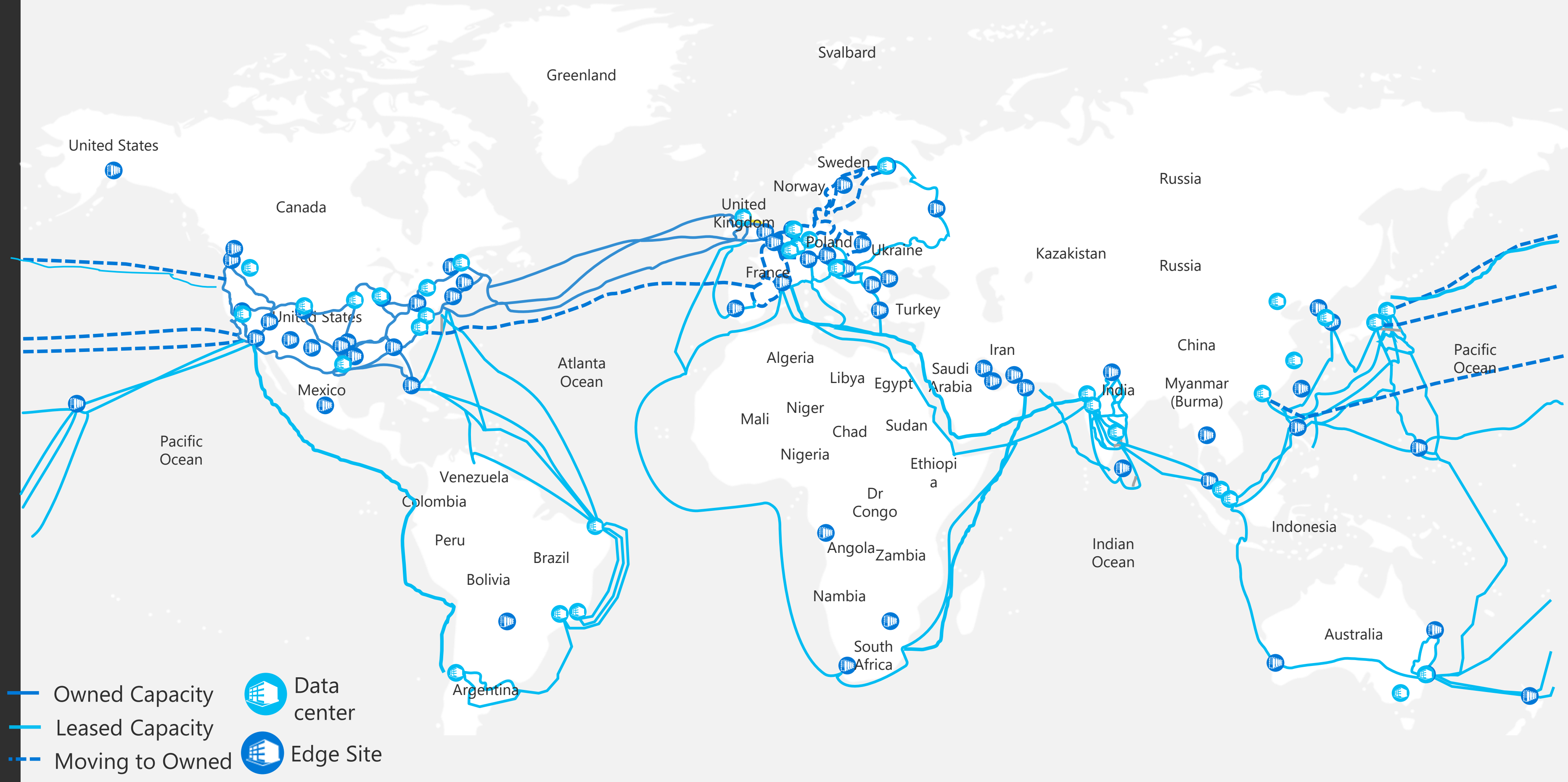
5 Performance & Monitoring

Microsoft Global Network

One of the largest private networks in the world

- 8,000+ ISP sessions
- 130+ edge sites
- 44 ExpressRoute locations
- 33,000 miles of lit fiber
- SDN Managed (SWAN, OLS)

DCs and Network sites not exhaustive



Microsoft Azure

Virtual Machine Networking

Virtual Machine Networking

IPv4 and IPv6 Support

Support for multiple network interfaces for routing and firewalls

Private and/or Public IP addresses (static or dynamic)

Network Security Groups for traffic isolation

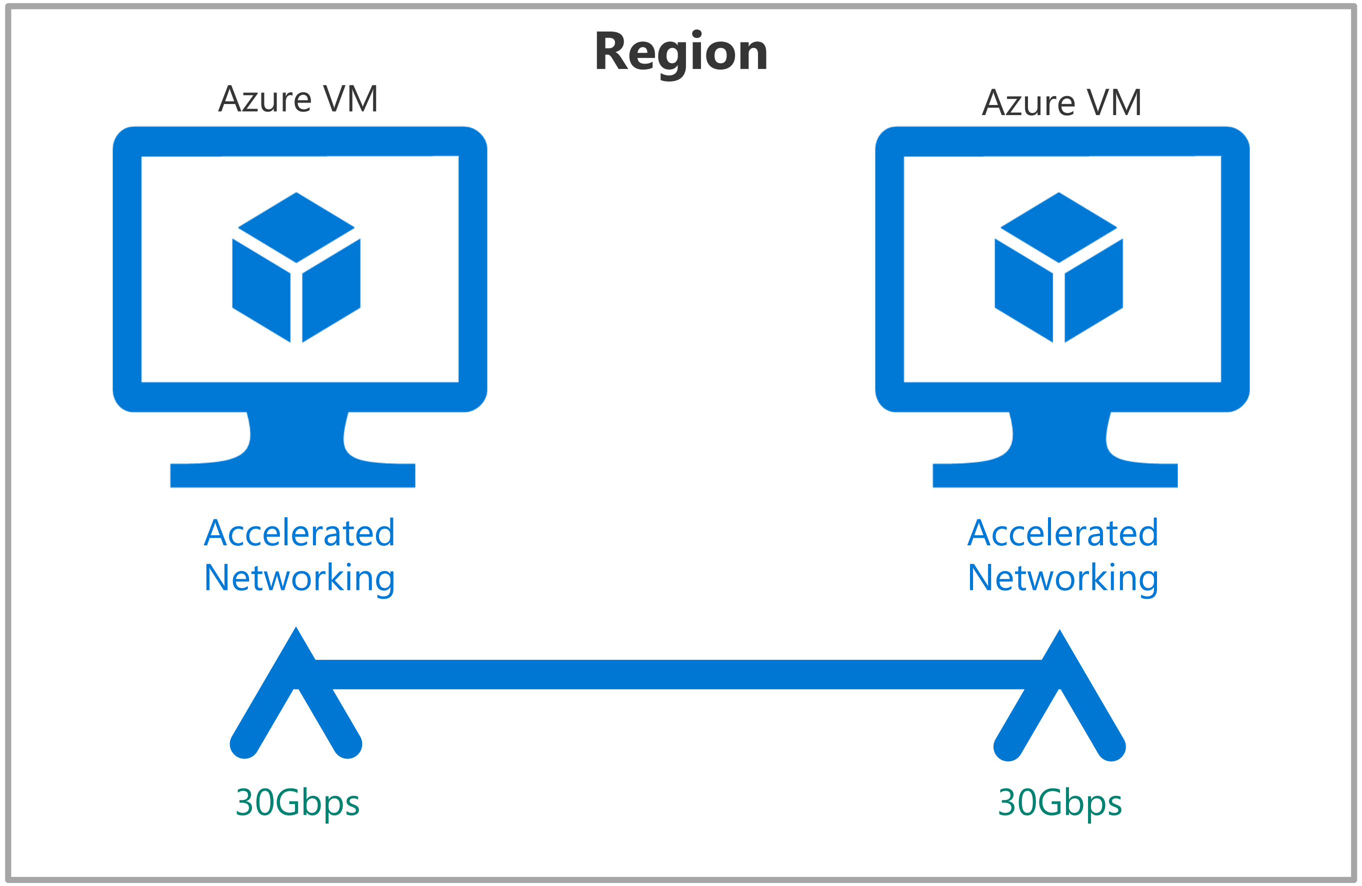
Automatic assignment of DNS servers from virtual network or from Azure DNS

Accelerated Networking

MAC Persistence

Accelerated Networking

30 Gbps VM to VM bandwidth!

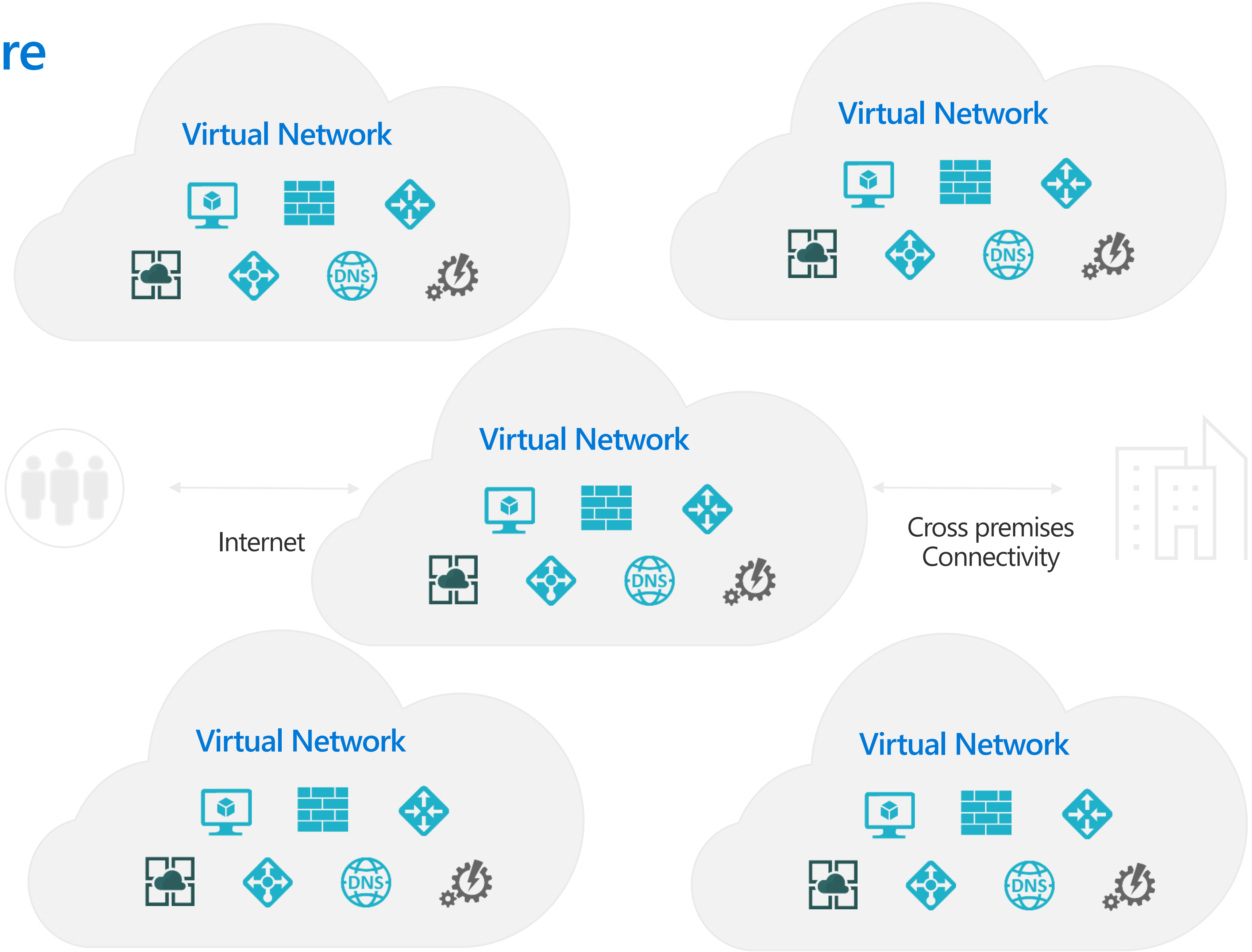


Your Network in Azure

Secure per customer virtual datacenter in the cloud

Instantiate and configure complex topologies in minutes

Rich security and networking services



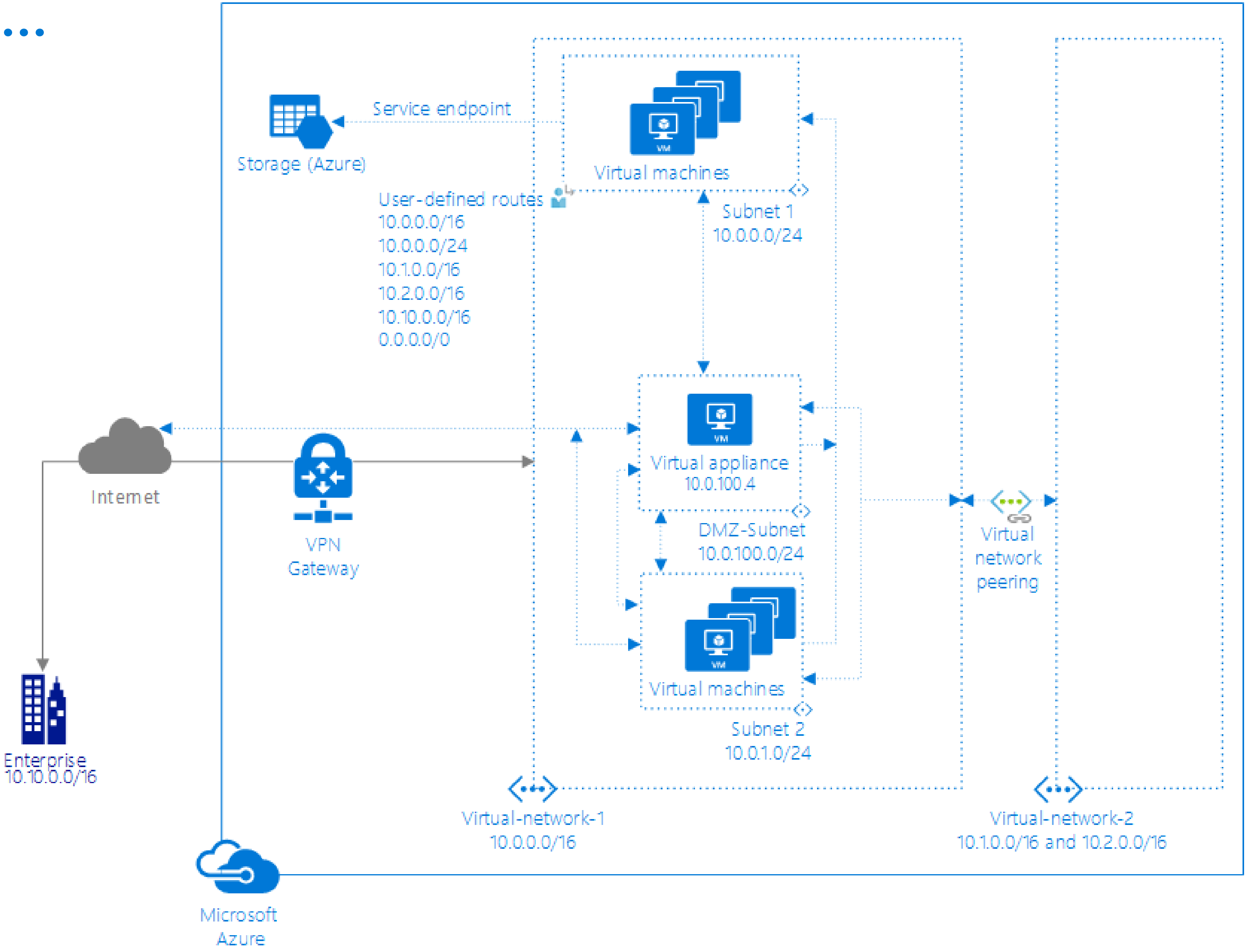
A typical configuration …

VNET

Subnet

IP Address

Public vs Private IPs



Microsoft Azure

Key Networking Services

Azure Networking Services

Distributed cloud connectivity

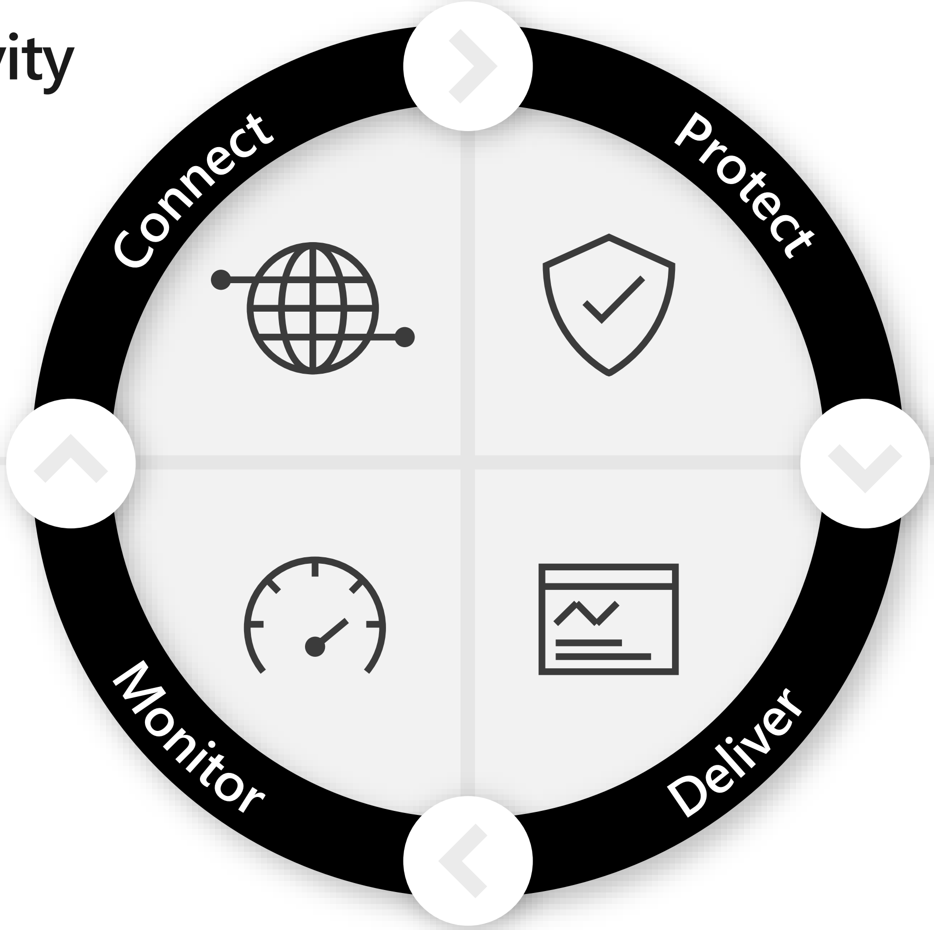
VNET

Virtual WAN

Express Route

VPN

DNS



Control and protect your cloud resources

DDoS

Firewall

NSG

WAF

VNET Endpoints

Measure – Monitor – Troubleshoot – Act

Azure Monitor

Network Monitor

Virtual Network TAP

Fast, secure and easy scaling of any web app

Load Balancer

Application Gateway

Traffic Manager

CDN

Front Door Service

Robust Network Services

Virtual Network

Provision private networks, optionally connect to on premise datacenters. NSG, User Defined Routes, & IP addresses.

Load Balancer

Deliver high availability and network performance to your applications

VPN Gateway

Establish secure, cross-premise connectivity

ExpressRoute

Dedicated private network fiber connections to Azure

Application Gateway/WAF

Build scalable and highly-available web front ends in Azure

DDoS Protection

Protect your Azure resources from DDoS attacks

Traffic Manager

Route incoming traffic for high performance and availability

Network Watcher

Network performance monitoring and diagnostics solution

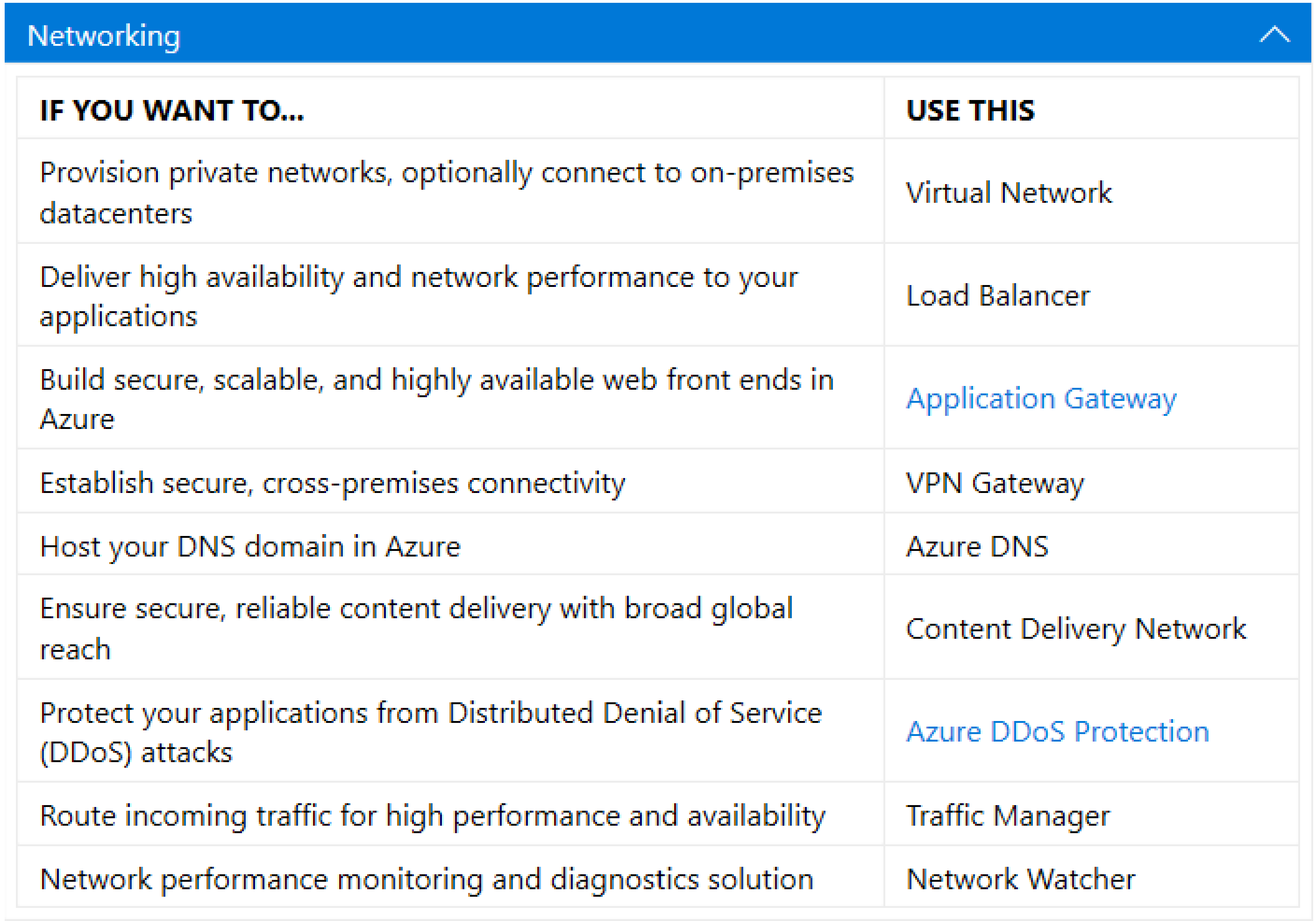
Azure DNS

Host your DNS domain in Azure

Content Delivery Network

Ensure secure, reliable content delivery with broad global reach

Which Networking Service Should I Use?



Networking

IF YOU WANT TO...	USE THIS
Provision private networks, optionally connect to on-premises datacenters	Virtual Network
Deliver high availability and network performance to your applications	Load Balancer
Build secure, scalable, and highly available web front ends in Azure	Application Gateway
Establish secure, cross-premises connectivity	VPN Gateway
Host your DNS domain in Azure	Azure DNS
Ensure secure, reliable content delivery with broad global reach	Content Delivery Network
Protect your applications from Distributed Denial of Service (DDoS) attacks	Azure DDoS Protection
Route incoming traffic for high performance and availability	Traffic Manager
Network performance monitoring and diagnostics solution	Network Watcher

Virtual Network

Azure Virtual Networks

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure.

Enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks.

Isolation and segmentation
Each vnet is isolated from other vnets by default.

Communicate with the internet
All resources in a virtual network can communicate outbound to the internet, by default.

Communicate between Azure resources
Through a virtual network.
Through a virtual network service endpoint.

Azure Virtual Networks

Virtual Network

Communicate with on-prem resources

Via P2S and S2S VPNs and ExpressRoute

Filter network traffic

Using Network security groups with security rules

Network virtual appliances

Route network traffic

Route tables

BGP routes

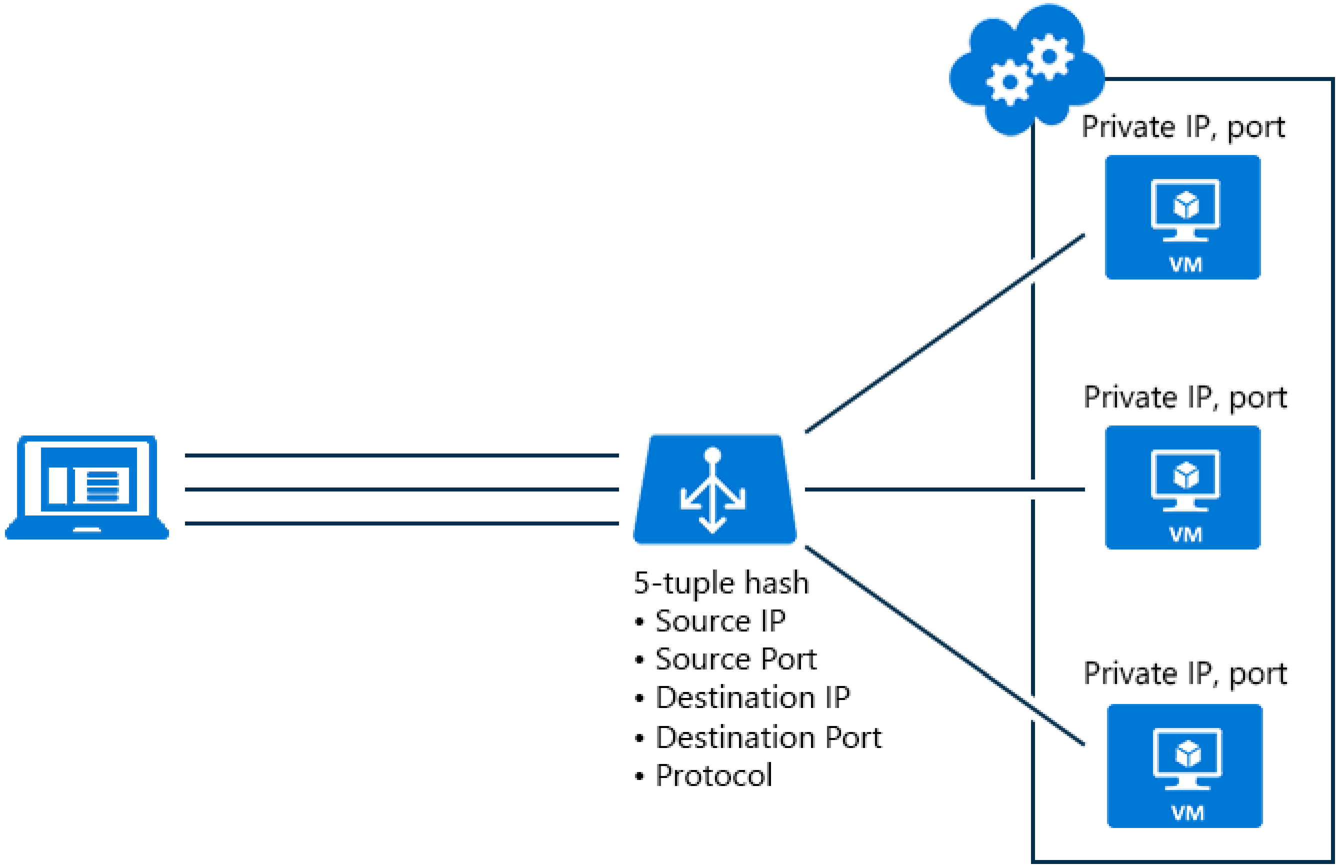
Load Balancer

Load Balancer

Operates at the transport layer (OSI layer 4 - TCP and UDP)

Distributes new inbound flows that arrive on the Load Balancer's frontend to backend pool instances, according to rules and health probes.

Azure Load Balancer is available in two SKUs: Basic and Standard. There are differences in scale, features, and pricing.



Load Balancer Rules and Health Probes

Rules

- Forward traffic from a specific port of a specific frontend IP address to a specific port of a specific backend instance.
- Common scenarios for this capability are Remote Desktop Protocol (RDP) or Secure Shell (SSH) sessions to individual VM instances inside the Azure Virtual Network.

Health probes

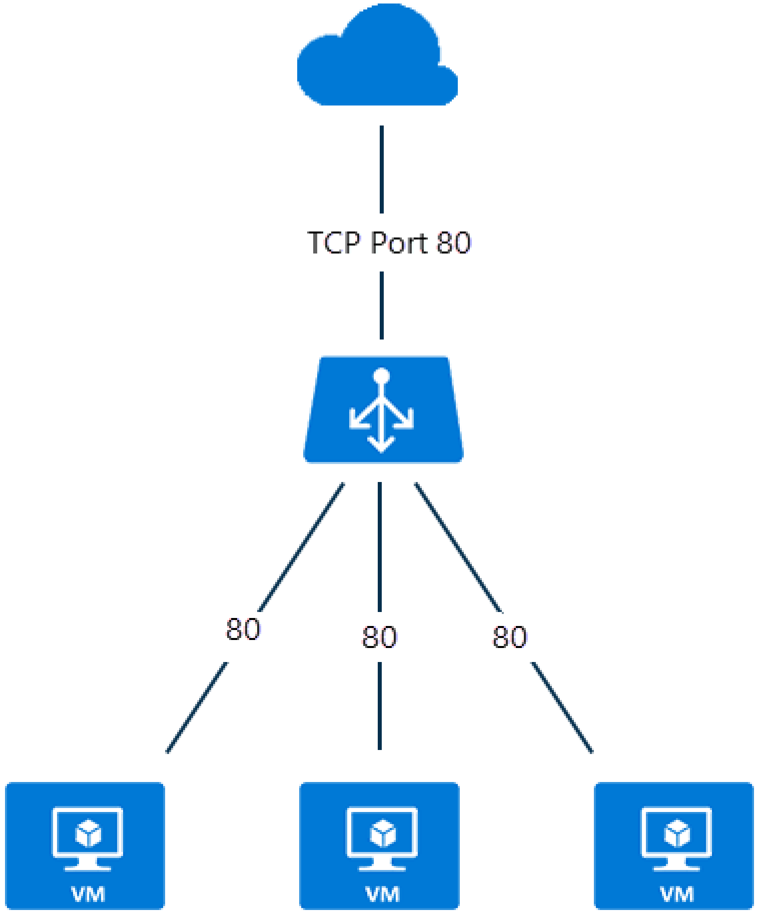
- Allow Load Balancer to detect the backend endpoint status.
- Determine which backend pool instances will receive new flow.
- When a health probe fails, Load Balancer will stop sending new flows to the respective unhealthy instance.
- Support multiple protocols including TCP, HTTP, and HTTPS

Load Balancer

Network Load Balancer – Public vs. Internal

A Public Load Balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the VM, and vice versa for the response traffic from the VM.

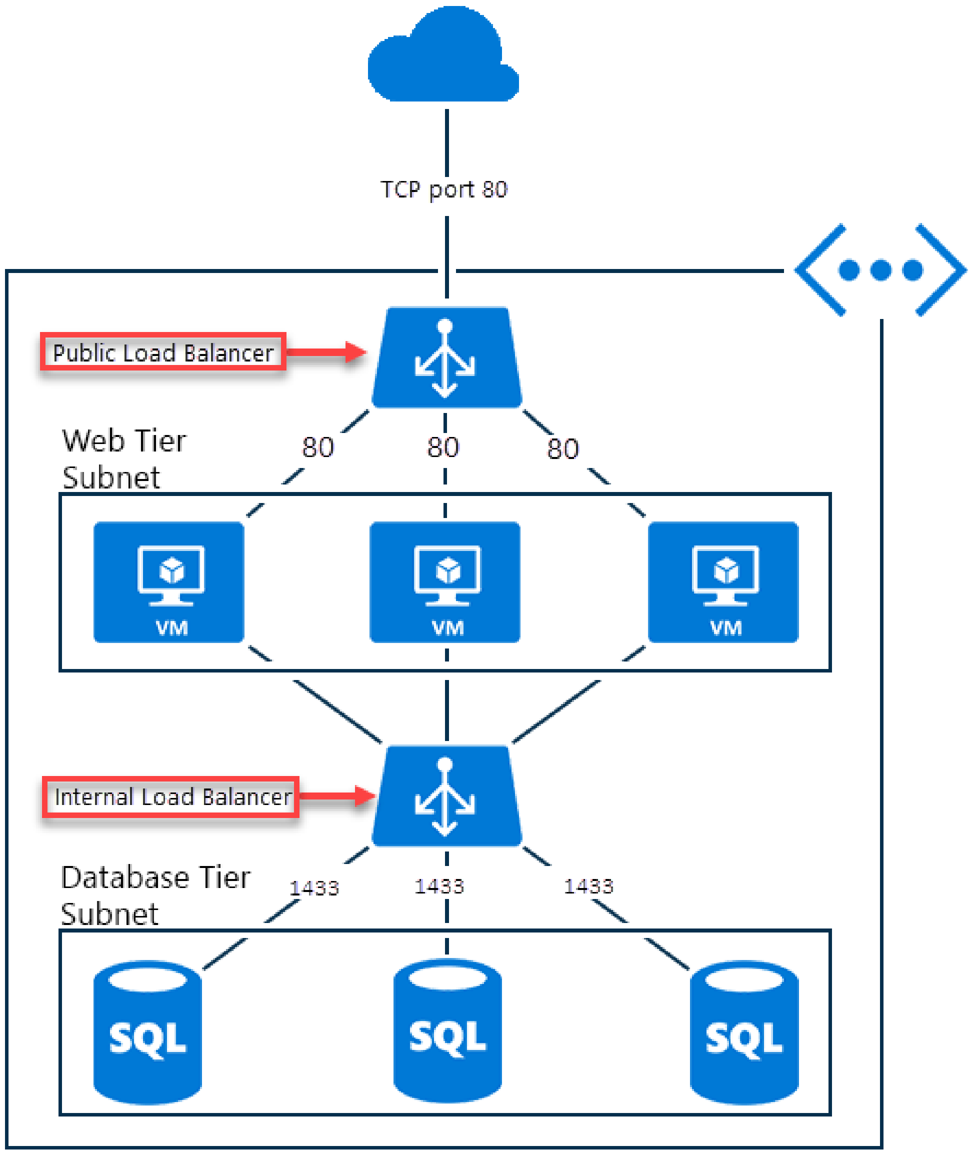
An Internal Load Balancer directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure. In this respect, an internal Load Balancer differs from a public Load Balancer.



Load Balancer

Load balancing multi-tier applications

Directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure.



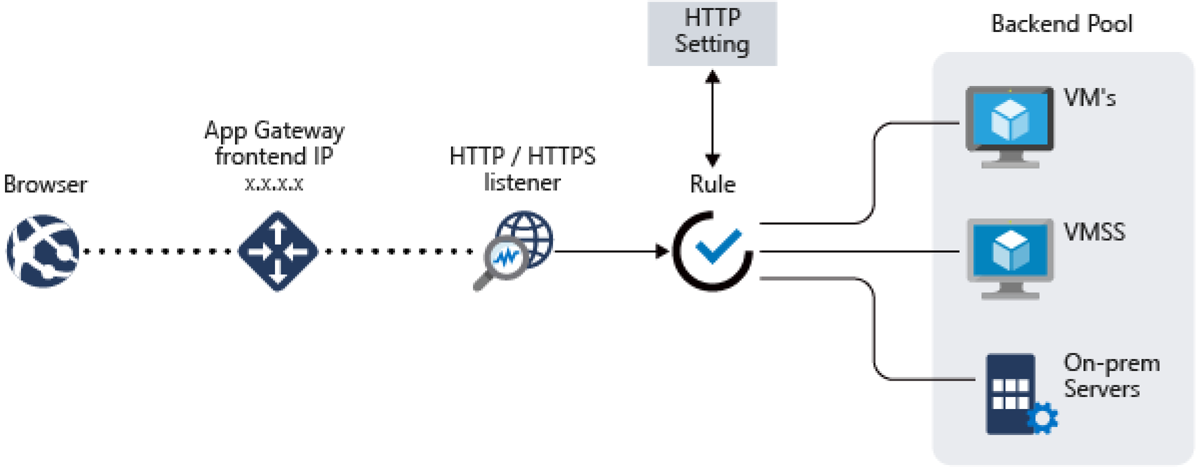
Azure Application Gateway

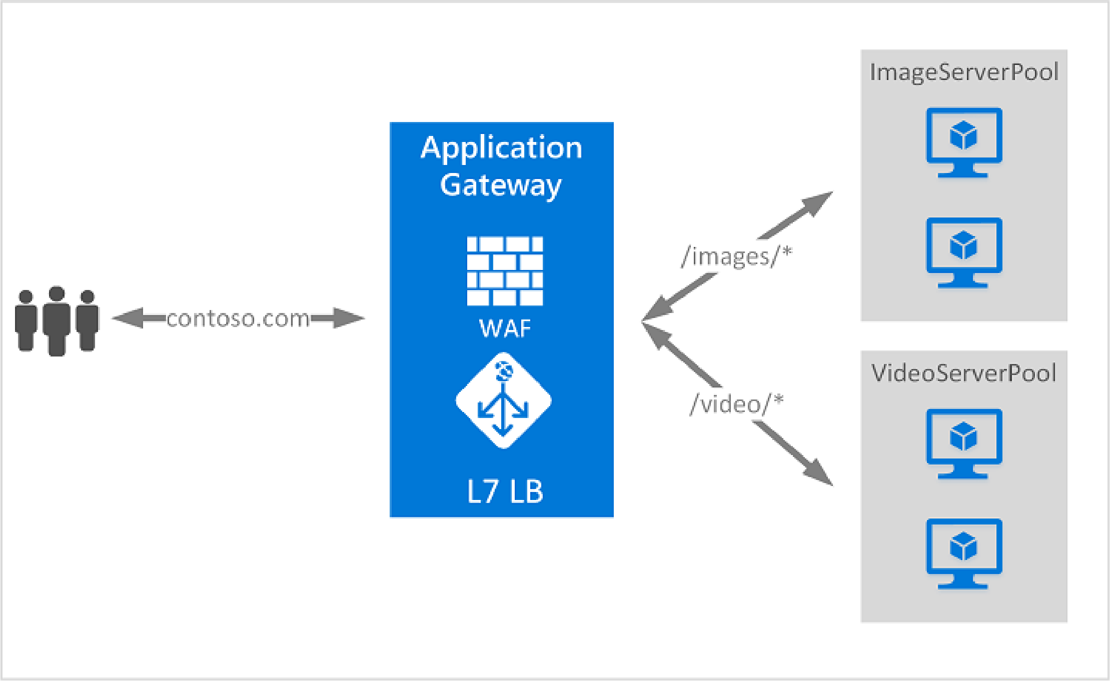
Web traffic load balancer that enables you to manage traffic to your **web** applications.

Performs application layer (OSI layer 7) load balancing and SSL termination.

Web application firewall based on rules from the [OWASP (Open Web Application Security Project) core rule sets](#) 3.0 or 2.2.9.

Application Gateway with WAF





Application Gateway Features

Application Gateway with WAF

Secure Sockets Layer (SSL/TLS) termination

allows web servers to be unburdened from costly encryption and decryption overhead

Autoscaling

Standard_v2 or WAF_v2 SKU support autoscaling and can scale up or down based on changing traffic load patterns

Zone redundancy

Standard_v2 or WAF_v2 SKU can span multiple Availability Zones

Web application firewall

provides centralized protection of your web applications from common exploits and vulnerabilities

Application Gateway Features (cont.)

Application Gateway with WAF

URL-based routing

allows you to route traffic to back-end server pools based on URL Paths of the request

Multiple-site hosting

enables you to configure more than one web site on the same application gateway instance

Redirection

automatic HTTP to HTTPS redirection to ensure all communication between an application and its users occurs over an encrypted path

Session affinity

cookie-based session affinity feature to keep a user session on the same server

Traffic Manager

A DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

There are several traffic routing methods available in Traffic Manager:

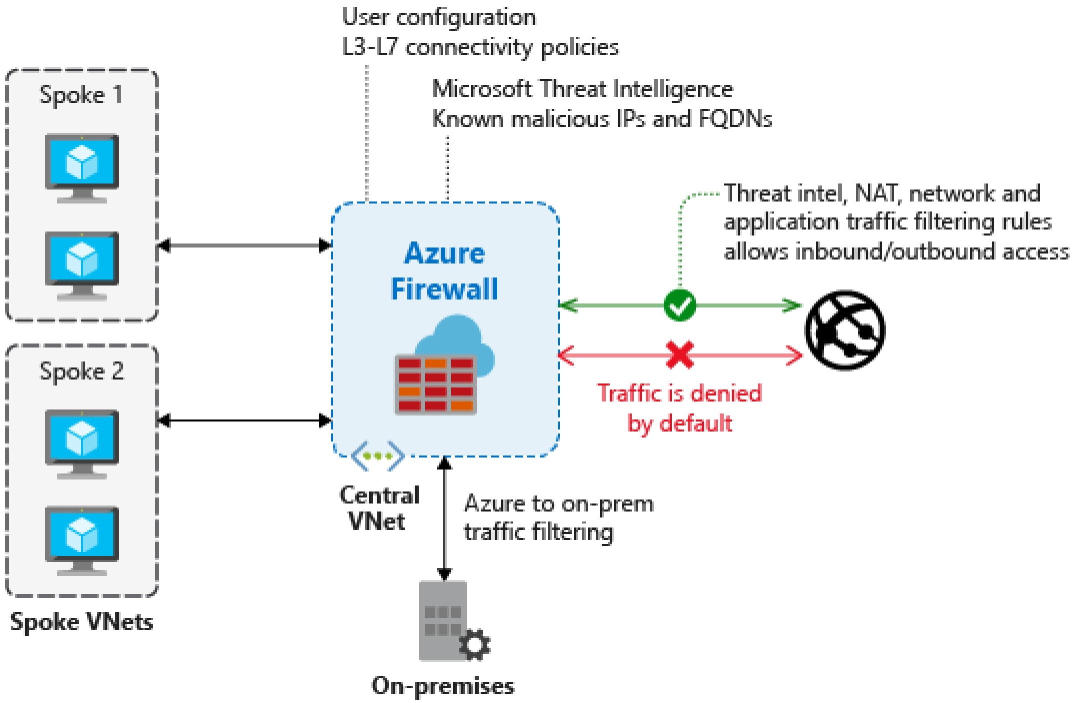
- Priority: use a primary service endpoint for all traffic
- Weighted: when you want to distribute traffic across a set of endpoints, either evenly or according to weights, which you define.
- Performance: when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint in terms of the lowest network latency.
- Geographic: users are directed to specific endpoints (Azure, External, or Nested) based on which geographic location their DNS query originates from.
- Multivalue: When a query is received for this profile, all healthy endpoints are returned.
- Subnet: map sets of end-user IP address ranges to a specific endpoint within a Traffic Manager profile.

Firewall

A managed, cloud-based network security service that protects your Azure Virtual Network resources.

It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

Centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks


User configuration
L3-L7 connectivity policies
Microsoft Threat Intelligence
Known malicious IPs and FQDNs
Spoke 1
Spoke 2
Spoke VNets
Azure Firewall
Threat intel, NAT, network and application traffic filtering rules allows inbound/outbound access
Traffic is denied by default
Central VNet
Azure to on-prem traffic filtering
On-premises

Azure DNS

Azure DNS

Hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure.

Can't use Azure DNS to buy a domain name.

Azure Private DNS

Provides a reliable, secure DNS service to manage and resolve domain names **in a virtual network** without the need to add a custom DNS solution.

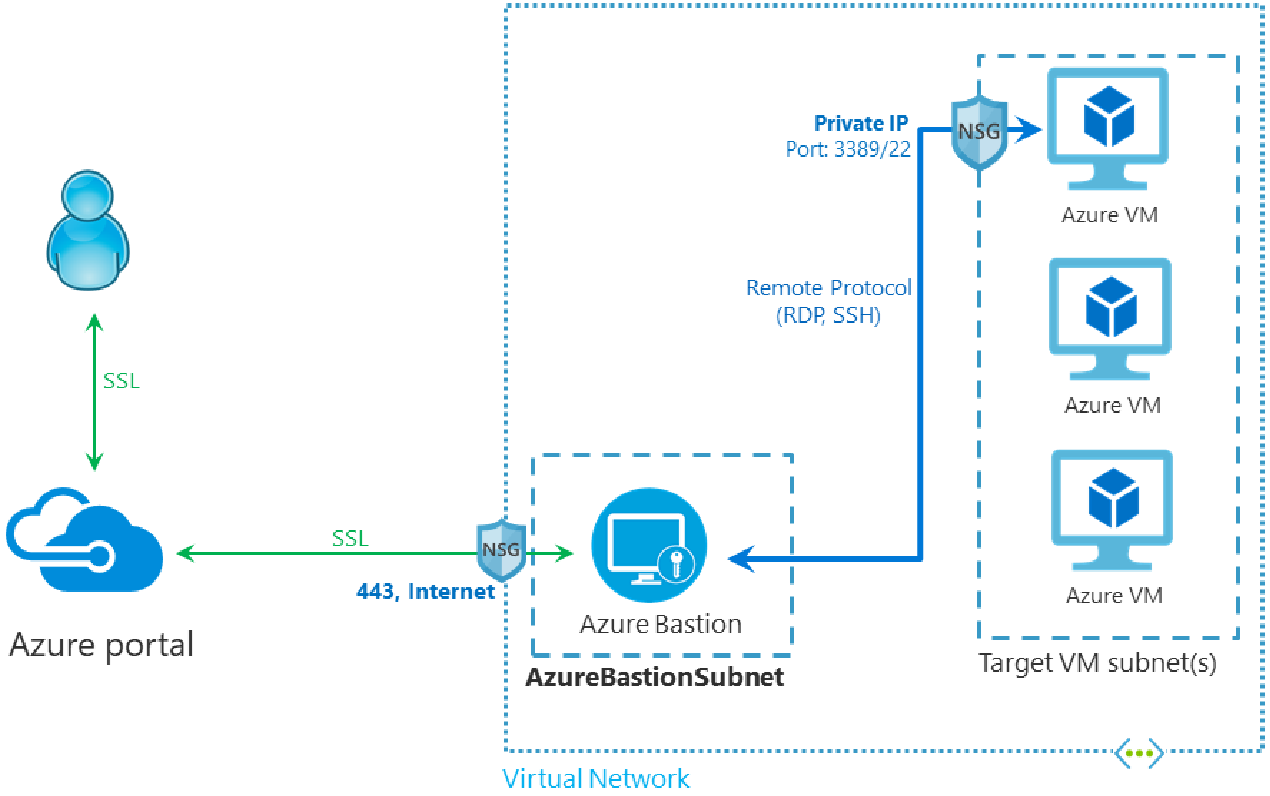
Can use your own custom domain names rather than the Azure-provided names available today.

Azure Bastion (Preview)

Secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over SSL.

When you connect via Azure Bastion, your virtual machines do not need a public IP address.

Bastion protects your virtual machines from exposing RDP/SSH ports to outside world while still providing secure access using RDP/SSH.



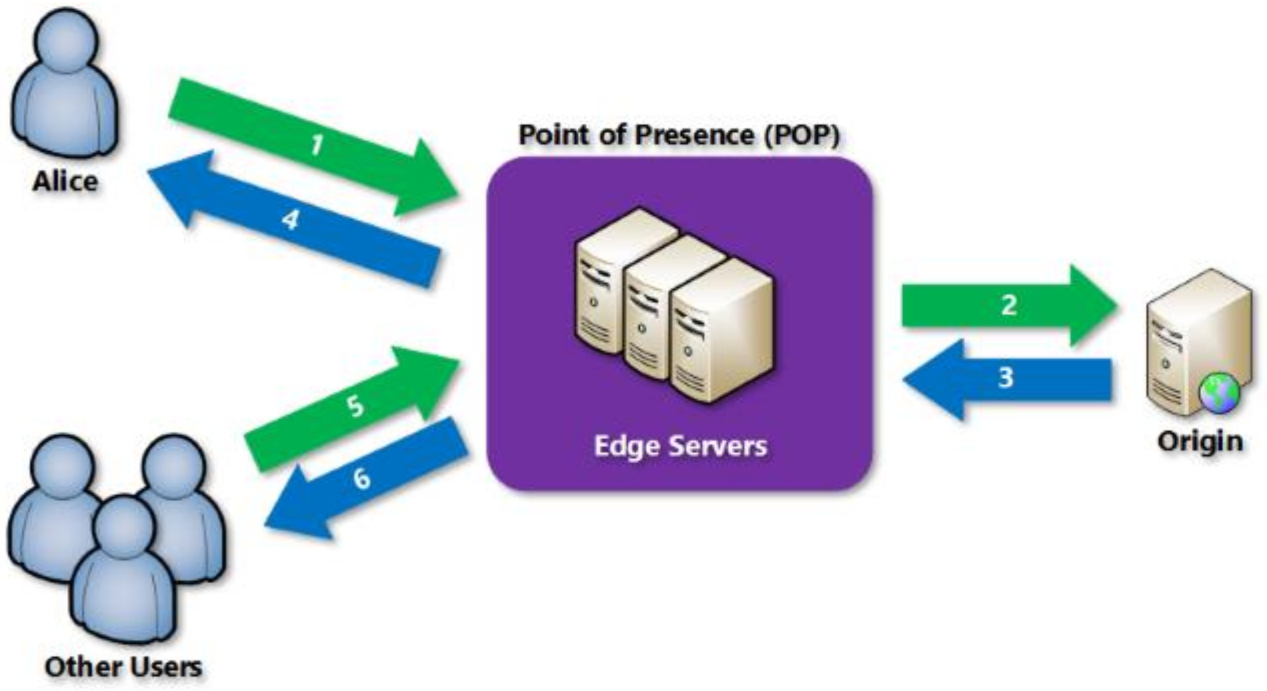
Azure Load Balancer v/s App Gateway v/s Traffic Manager v/s Front Door

Azure provides a suite of fully managed load-balancing solutions for your scenarios. Front Door provides a range of traffic-routing methods and backend health monitoring options to suit different application needs and automatic failover models. If you are looking for a DNS based global routing and do **not** have requirements for Transport Layer Security (TLS) protocol termination ("SSL offload") or per-HTTP/HTTPS request, application-layer processing, review **Traffic Manager**. If you are looking for load balancing between your servers in a region, for application layer, review **Application Gateway** and for network layer load balancing, review **Load Balancer**. Your end-to-end scenarios might benefit from combining these solutions as needed.

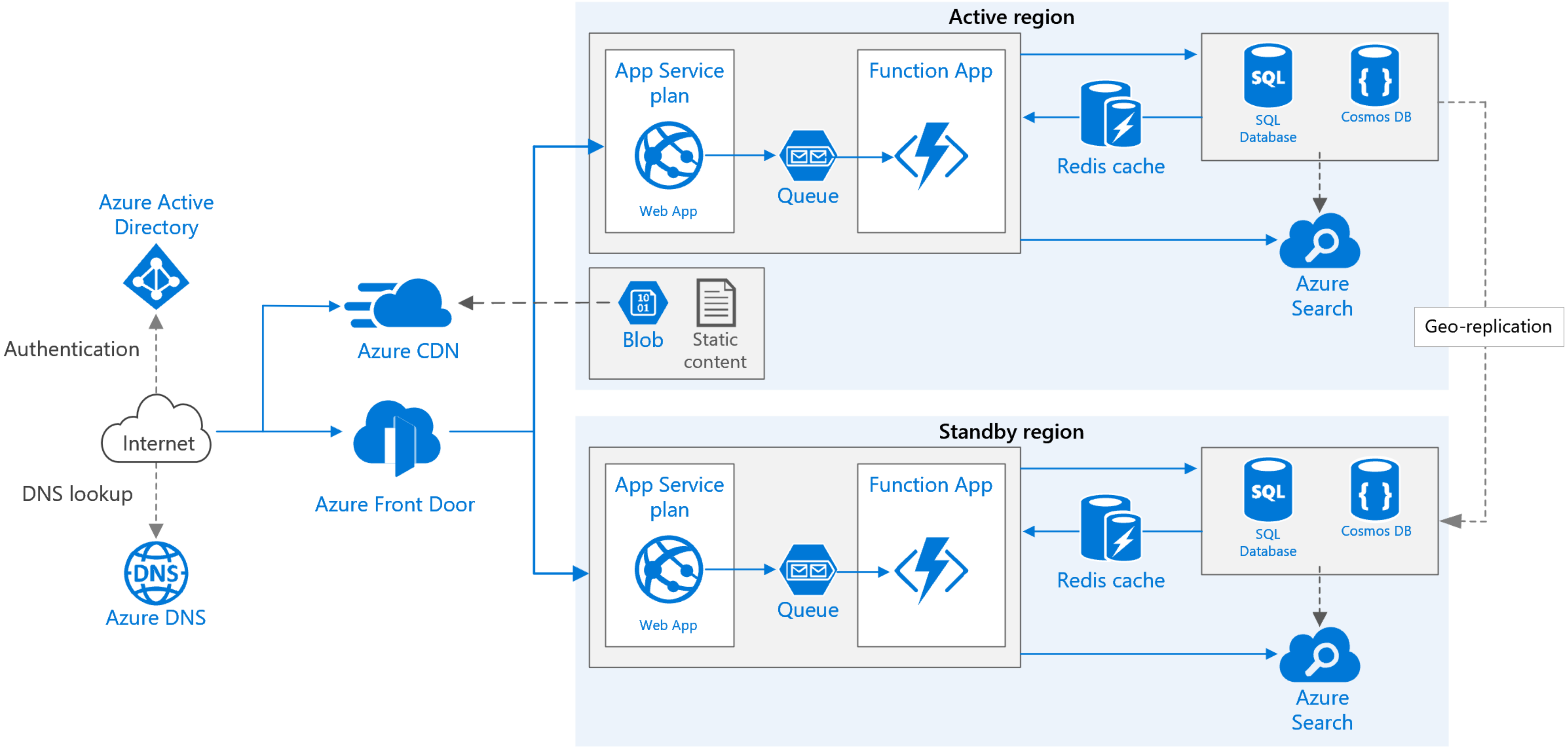
Good comparison sans Front Door:
http://www.prosdn.com/azure-load-balancer-vs-app-gateway-vs-traffic-manager/

Content Delivery Network

A distributed network of servers that can efficiently deliver web content to users. CDNs store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.



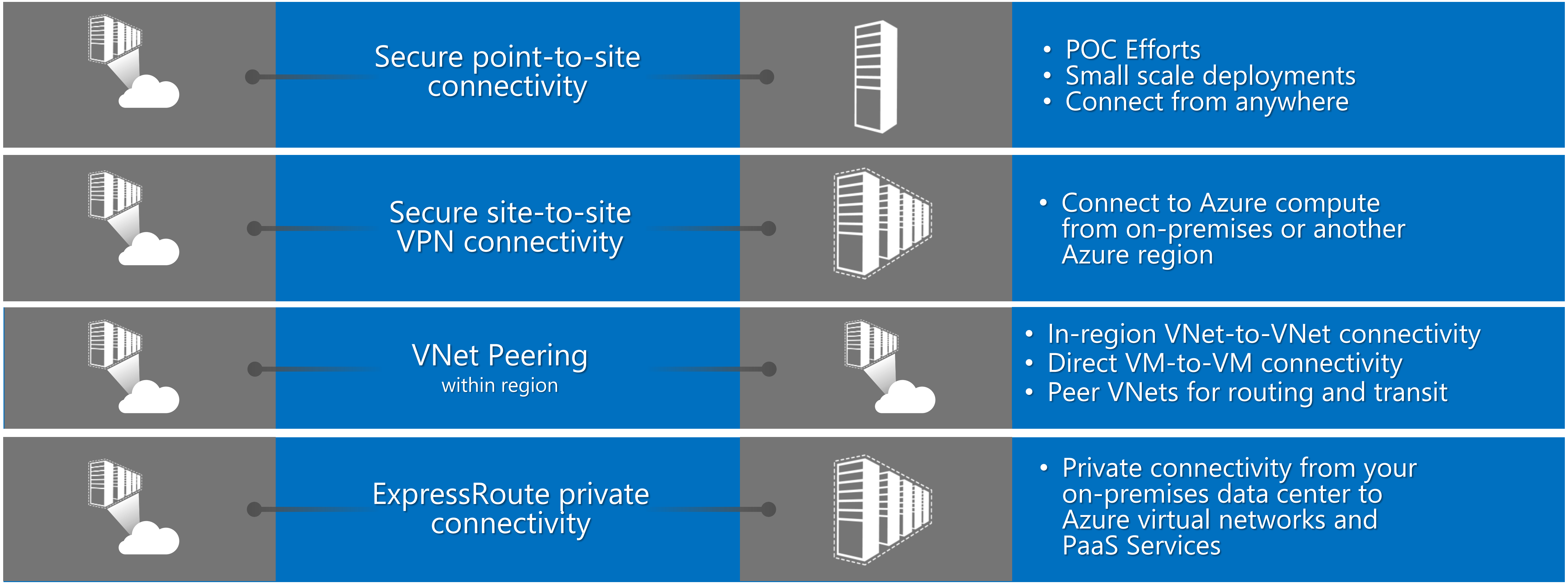
Combining Services ...



Microsoft Azure

Hybrid Networking

Hybrid Connectivity



Secure point-to-site connectivity

- POC Efforts
- Small scale deployments
- Connect from anywhere

Secure site-to-site VPN connectivity

- Connect to Azure compute from on-premises or another Azure region

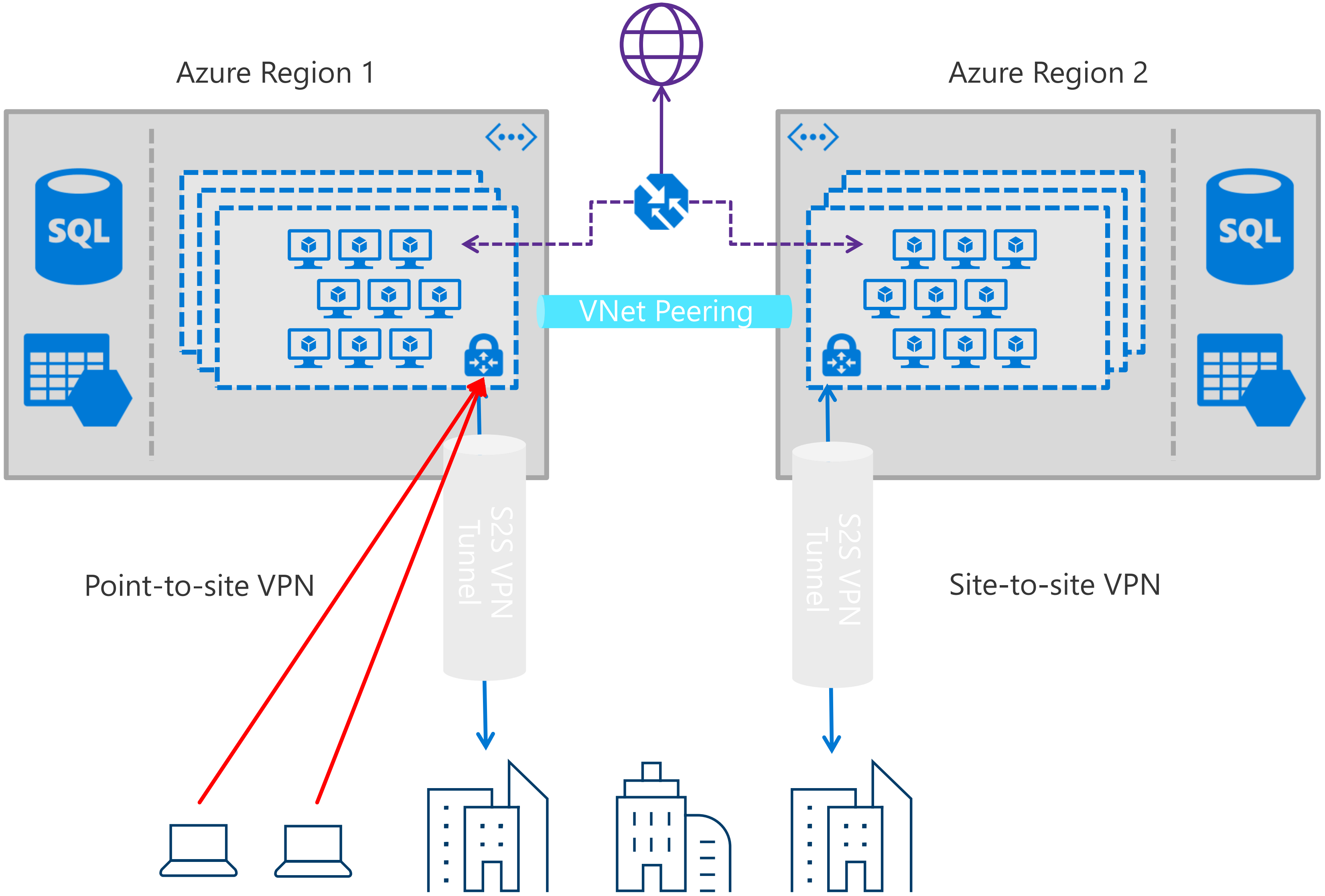
VNet Peering
within region

- In-region VNet-to-VNet connectivity
- Direct VM-to-VM connectivity
- Peer VNets for routing and transit

ExpressRoute private connectivity

- Private connectivity from your on-premises data center to Azure virtual networks and PaaS Services

VPN and Point-to-site (P2S)



ExpressRoute

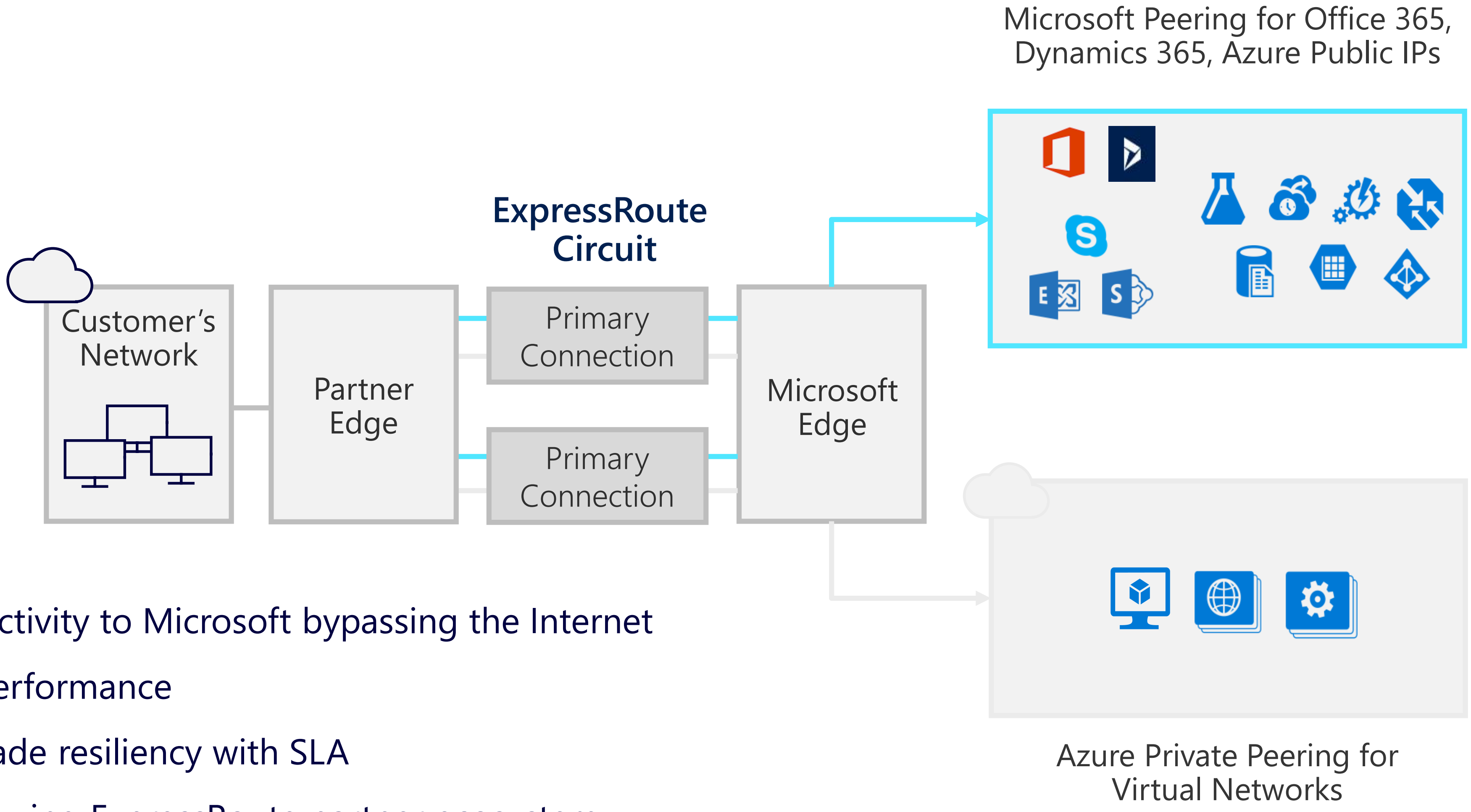
Fast, private connection to Microsoft cloud services from your on-premises infrastructure or colocation facility.

Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider.

Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.

https://azure.microsoft.com/en-us/services/expressroute/

ExpressRoute



Private connectivity to Microsoft bypassing the Internet

Predictable performance

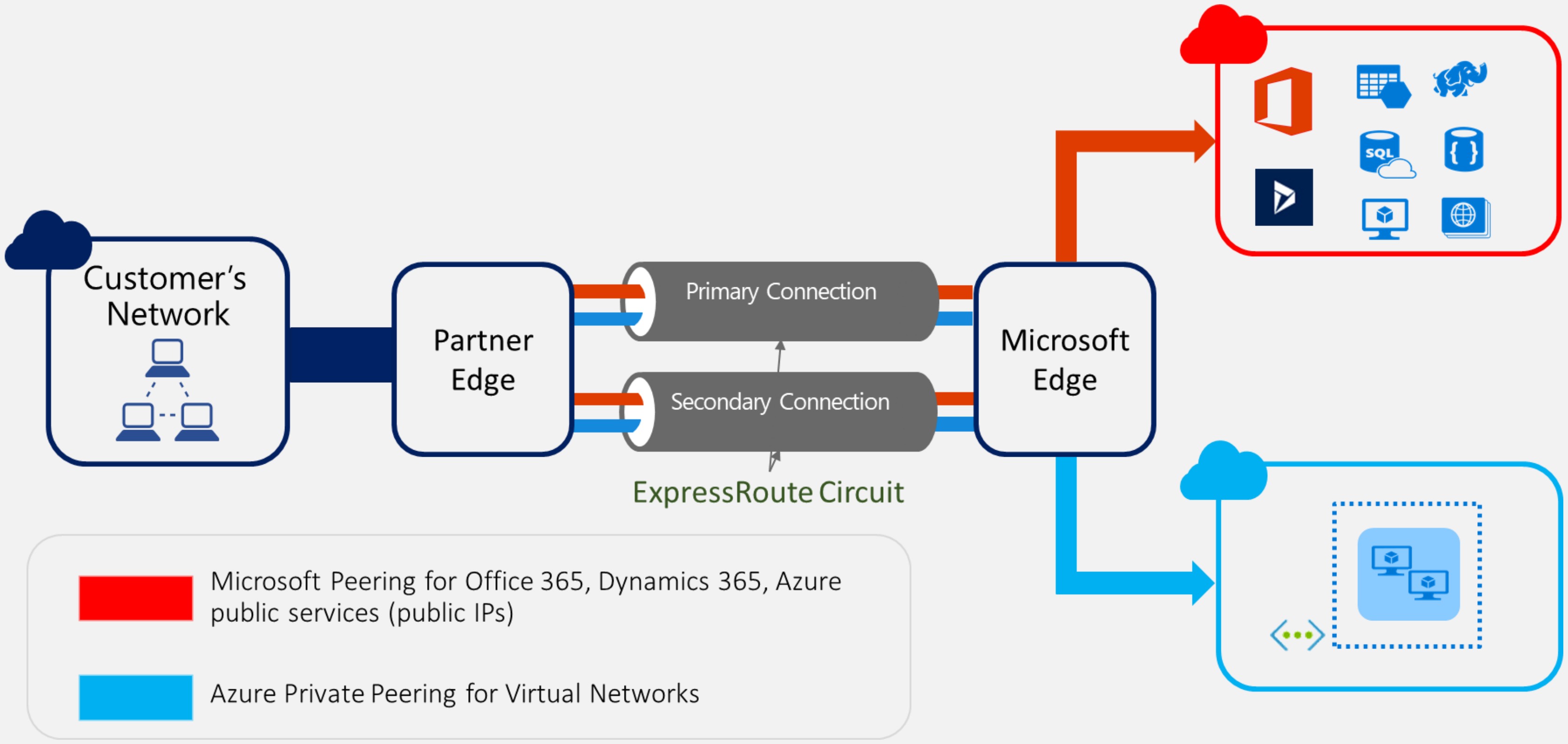
Enterprise-grade resiliency with SLA

Large and growing ExpressRoute partner ecosystem

Azure Network Framework

UDRs - User Defined Routes

VPN/ExpressRoute



🟥 Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)

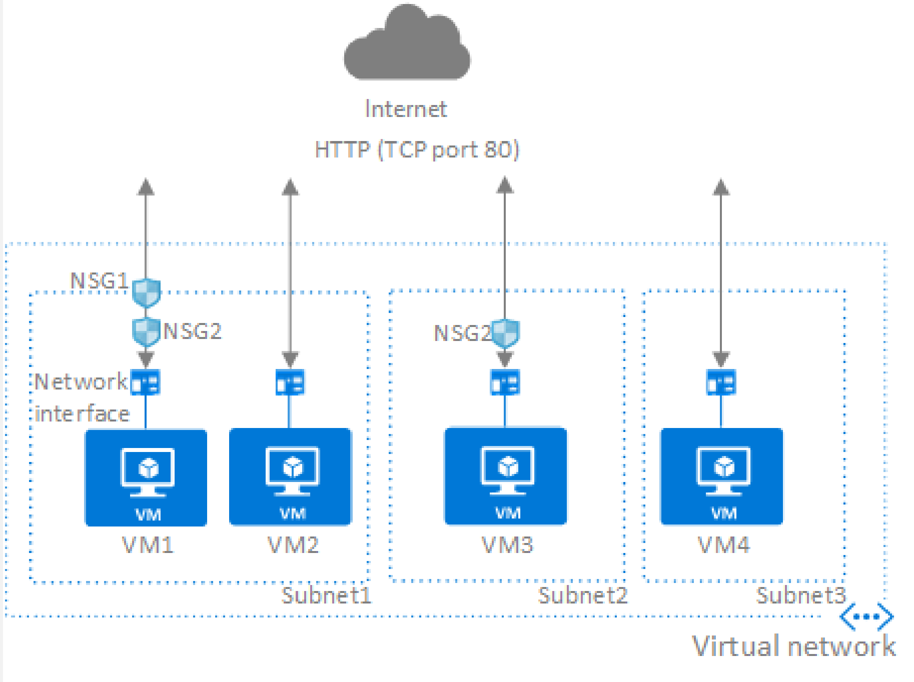
🟦 Azure Private Peering for Virtual Networks

Azure Network Framework

NSG (Network Security Groups)

Service Tags

Application Security Groups

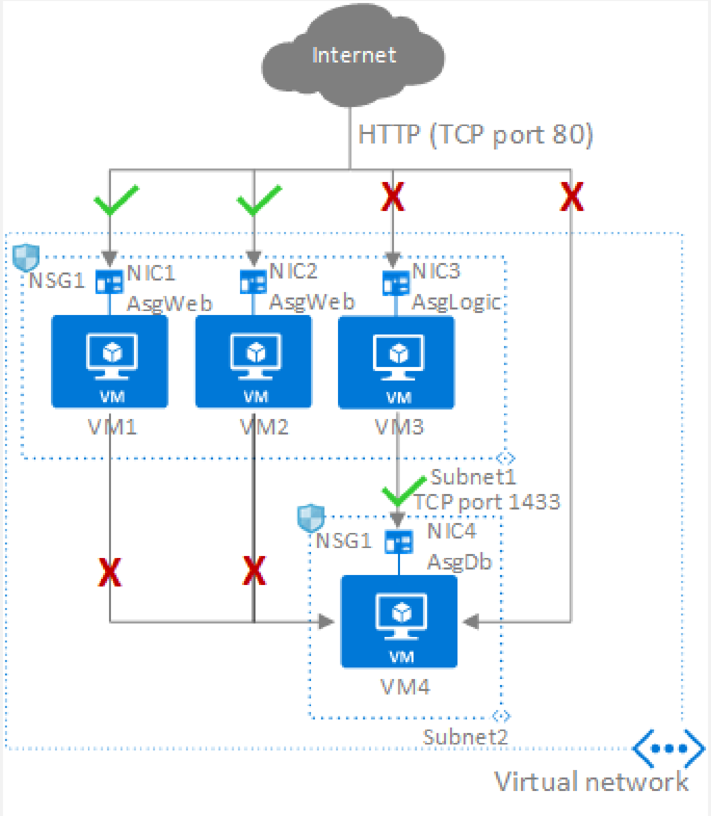


NSGs

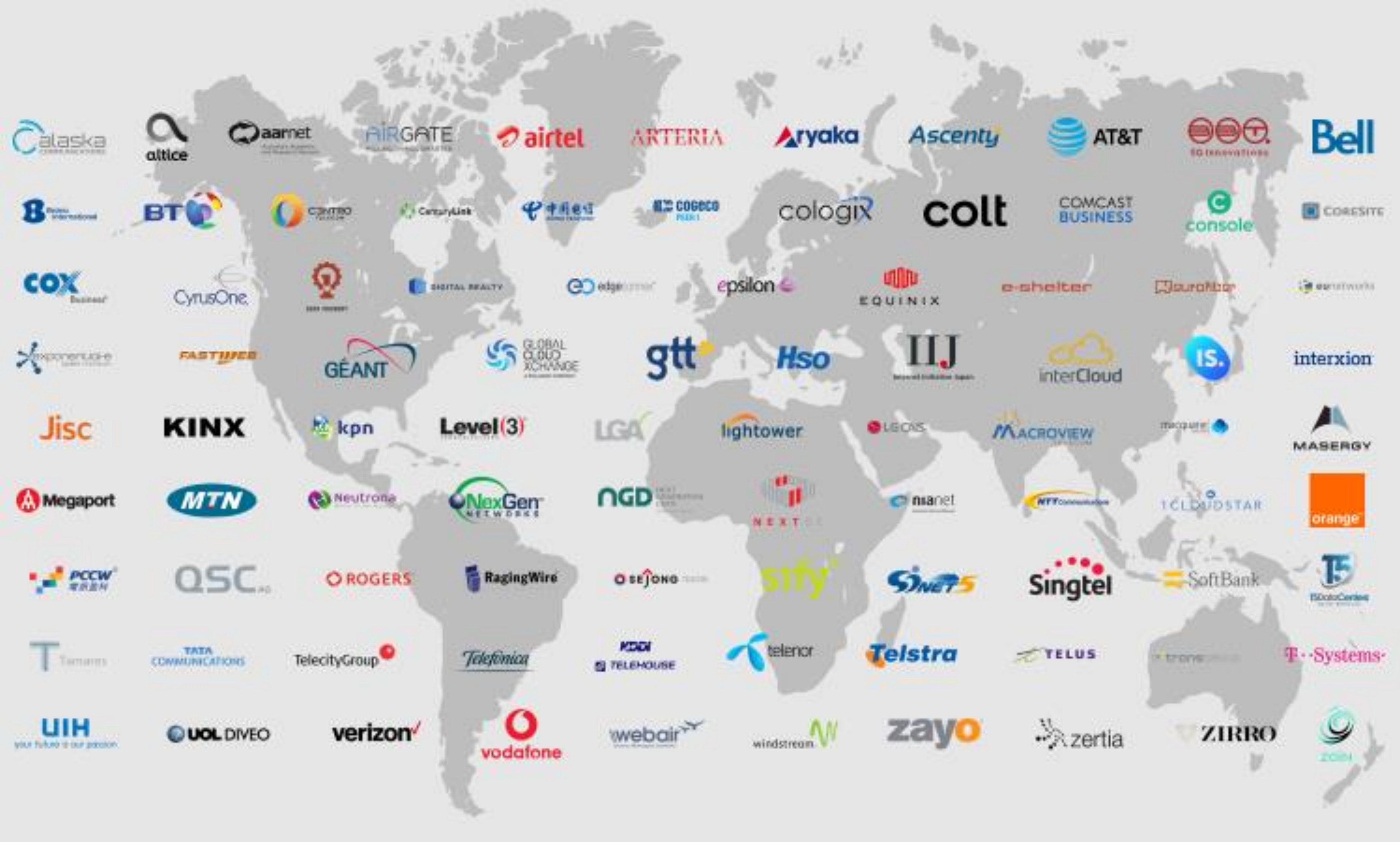
- Prioritized Inbound/Outbound Rules
- Assigned to NIC or Subnet
- Default Security Rules

NSG Options

- Augmented Security Rules
- Service Tags
- Application Security Groups



ExpressRoute | 200+ Partners



Microsoft Azure

Performance & Monitoring

Monitoring landscape – Apps & Infrastructure

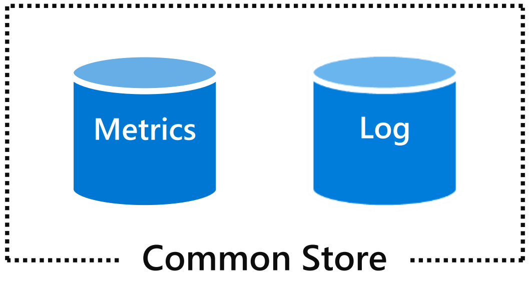
Infrastructure

Apps

Network

Azure Monitor

Full observability for your infra, app and network



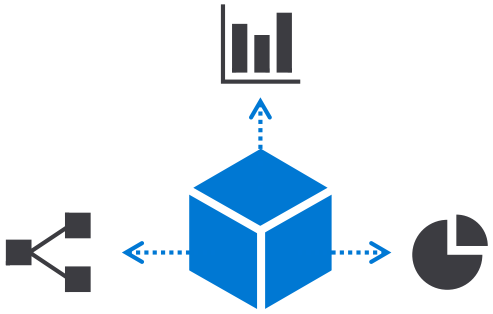
Metrics

Log

Common Store

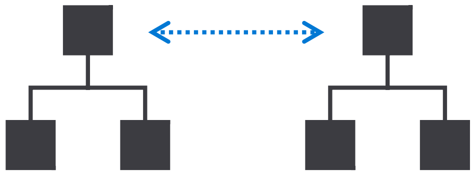
Unified monitoring

A common platform for all metrics, logs and other monitoring telemetry



Data driven insights

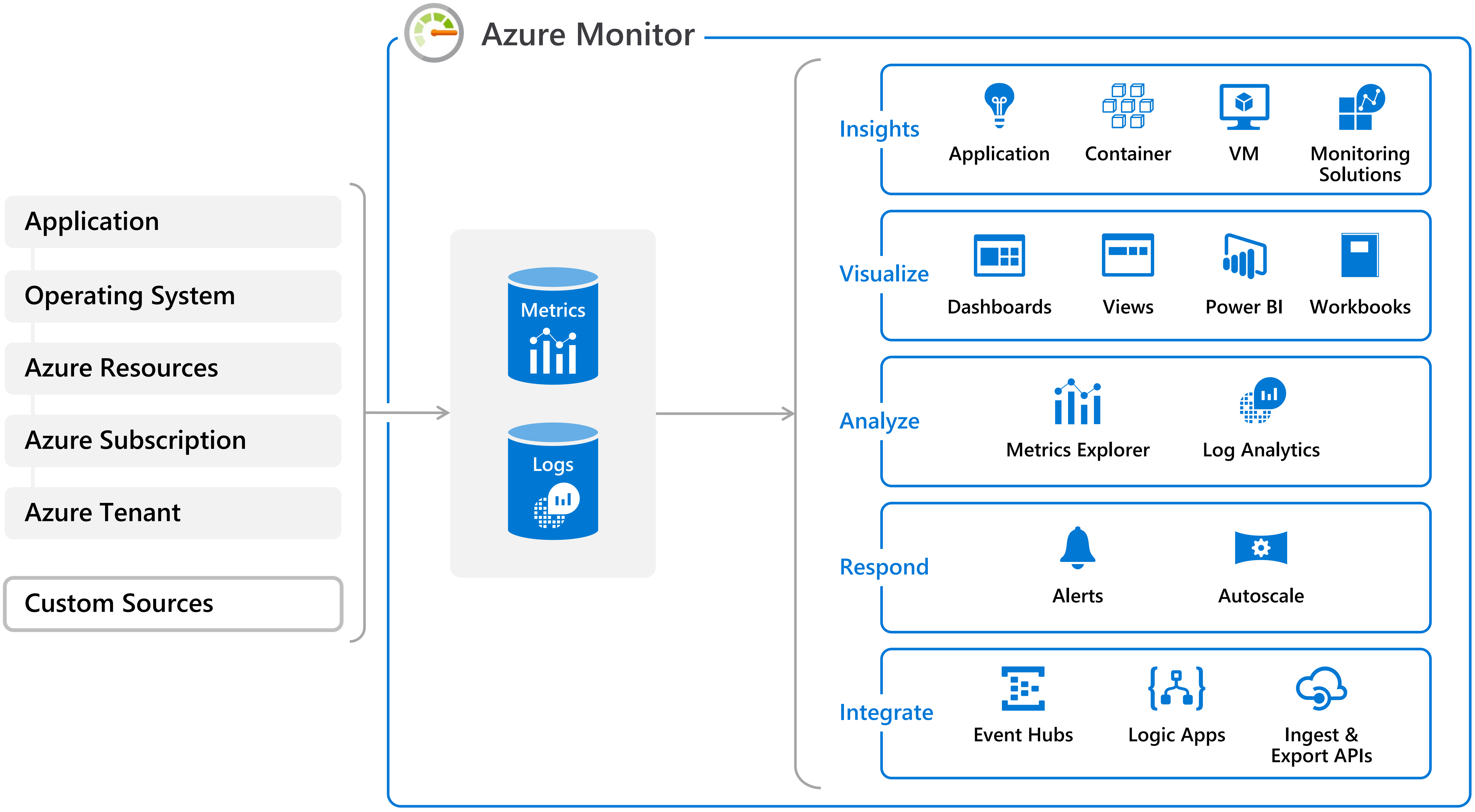
Advanced querying and analytics powered by machine learning capabilities



Partner integrations

Rich ecosystem of popular DevOps, issue management, SIEM, and ITSM tools

Includes Application Insights & Log Analytics


Azure Monitor
Application
Operating System
Azure Resources
Azure Subscription
Azure Tenant
Custom Sources
Metrics
Logs
Insights
Application
Container
VM
Monitoring Solutions
Visualize
Dashboards
Views
Power BI
Workbooks
Analyze
Metrics Explorer
Log Analytics
Respond
Alerts
Autoscale
Integrate
Event Hubs
Logic Apps
Ingest & Export APIs

Network Watcher

Network Watcher

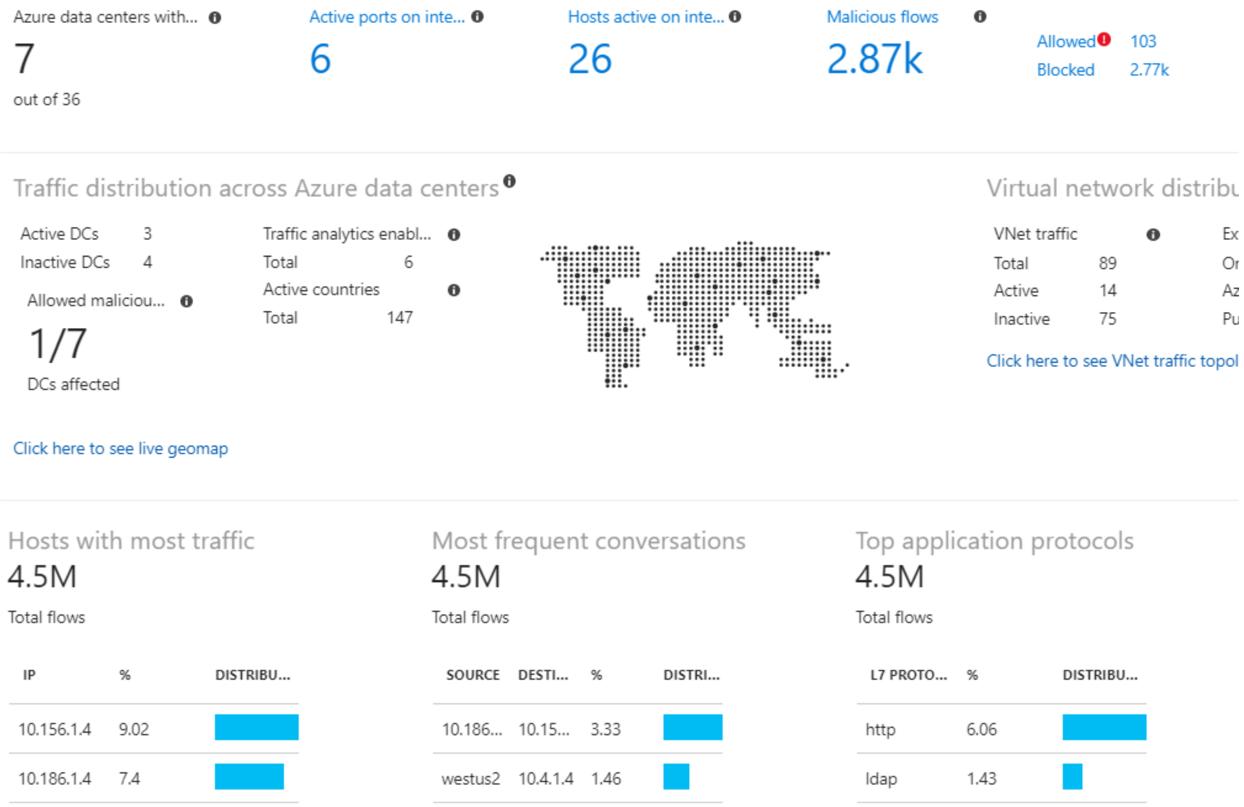
Network Watcher

Provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.

Monitor communication between a virtual machine and an endpoint.

Diagnose network traffic filtering problems to or from a VM.

Diagnose outbound connections from a VM
Capture packets to and from a VM.



Azure data centers with... 7 out of 36

Active ports on inte... 6

Hosts active on inte... 26

Malicious flows 2.87k

Allowed	103
Blocked	2.77k

Traffic distribution across Azure data centers

Active DCs	3
Inactive DCs	4

Allowed maliciou... 1/7 DCs affected

Traffic analytics enabl...

Total	6

Active countries

Total	147

Click here to see live geomap

Virtual network distribu

VNet traffic

Total	89
Active	14
Inactive	75

Ex
Or
Az
Pu

Click here to see VNet traffic topol

Hosts with most traffic
4.5M
Total flows

IP	%	DISTRIBU...
10.156.1.4	9.02	
10.186.1.4	7.4	

Most frequent conversations
4.5M
Total flows

SOURCE	DESTI...	%	DISTRI...
10.186...	10.15...	3.33	
westus2	10.4.1.4	1.46	

Top application protocols
4.5M
Total flows

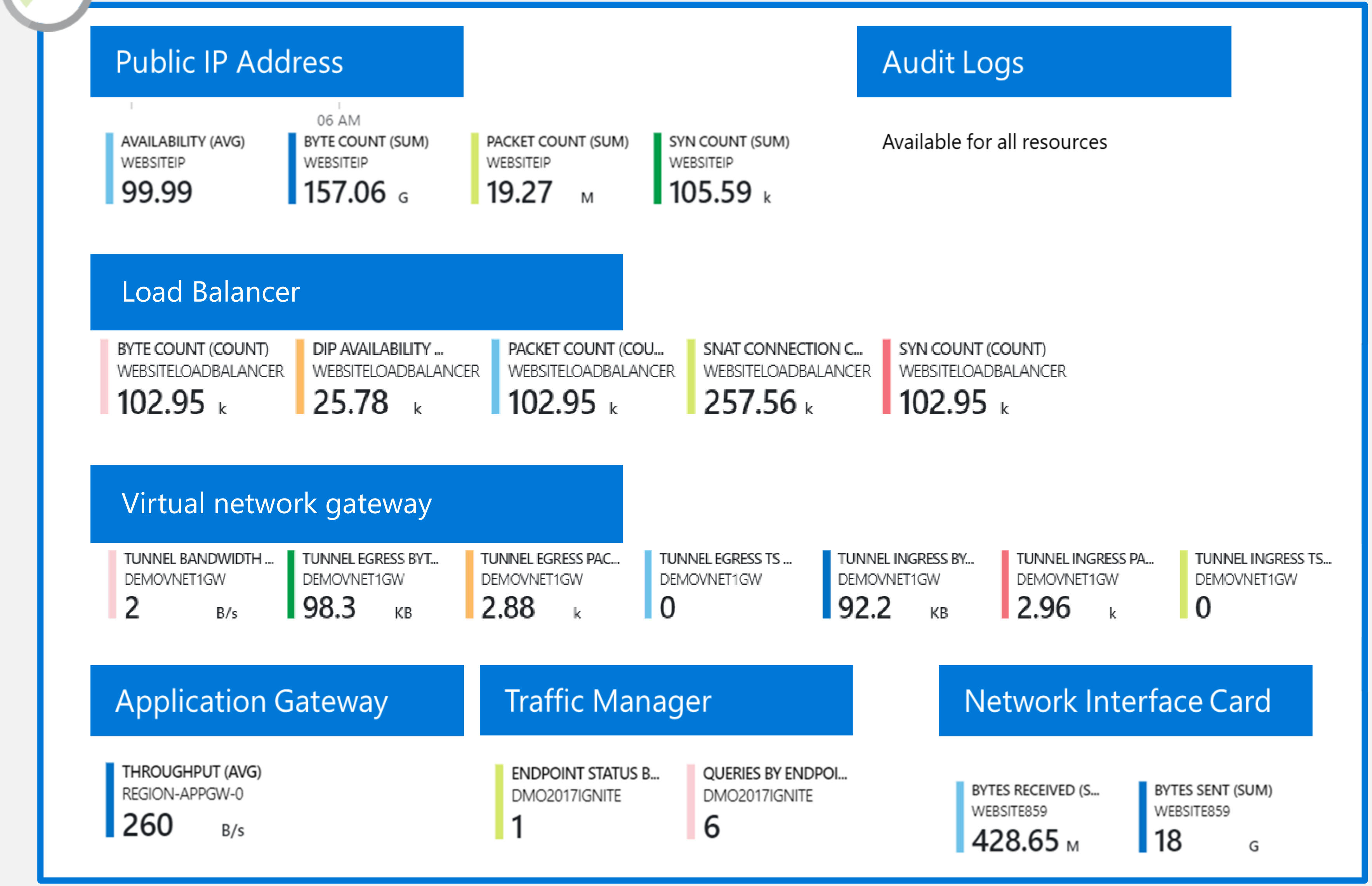
L7 PROTO...	%	DISTRIBU...
http	6.06	
ldap	1.43	

Performance and Monitoring

Performance

Monitoring

Monitoring your resources with Azure Monitor



Public IP Address

06 AM

AVAILABILITY (AVG)
WEBSITEIP
99.99

BYTE COUNT (SUM)
WEBSITEIP
157.06 G

PACKET COUNT (SUM)
WEBSITEIP
19.27 M

SYN COUNT (SUM)
WEBSITEIP
105.59 k

Audit Logs

Available for all resources

Load Balancer

BYTE COUNT (COUNT)
WEBSITELOADBALANCER
102.95 k

DIP AVAILABILITY ...
WEBSITELOADBALANCER
25.78 k

PACKET COUNT (COU...
WEBSITELOADBALANCER
102.95 k

SNAT CONNECTION C...
WEBSITELOADBALANCER
257.56 k

SYN COUNT (COUNT)
WEBSITELOADBALANCER
102.95 k

Virtual network gateway

TUNNEL BANDWIDTH ...
DEMOVNET1GW
2 B/s

TUNNEL EGRESS BYT...
DEMOVNET1GW
98.3 KB

TUNNEL EGRESS PAC...
DEMOVNET1GW
2.88 k

TUNNEL EGRESS TS ...
DEMOVNET1GW
0

TUNNEL INGRESS BY...
DEMOVNET1GW
92.2 KB

TUNNEL INGRESS PA...
DEMOVNET1GW
2.96 k

TUNNEL INGRESS TS...
DEMOVNET1GW
0

Application Gateway

THROUGHPUT (AVG)
REGION-APPGW-0
260 B/s

Traffic Manager

ENDPOINT STATUS B...
DMO2017IGNITE
1

QUERIES BY ENDPOI...
DMO2017IGNITE
6

Network Interface Card

BYTES RECEIVED (S...
WEBSITE859
428.65 M

BYTES SENT (SUM)
WEBSITE859
18 G

Microsoft Azure

Questions?